KOD
LATAM
SECURITY

Virtual Data Protection

Una herramienta para la protección de los entornos de virtualización en base a VMware vSphere y Microsoft Hyper-V

VENTAJAS

- Apoyo de las plataformas más comunes de virtualización VMware vSphere y Microsoft Hyper-V
- Auditoria sobre las actividades de los administradores de la infraestructura virtual
- Gestión de cambios y control de integridad sobre ambientes virtuales
- Cumplimiento regulatorio sobre ambientes virtuales

Virtual
Data
Protection

FUNCIONALIDADES

Soporte para infraestructuras distribuidas

- Capacidad de alta disponibilidad.
- Soporte de múltiples servidores vCenter, combinados con el modo de VMware vCenter Linked Mode.
- Conexión del agente de autenticación a varios servidores de autorización de VDP R2.
- Creacón del forest para los servidores de autorización de VDP R2.
- Control de gestión de Microsoft Hyper-V a través de System Center Virtual Machine Manager y Failover Cluster Manager.

Diferenciación sobre el acceso a la gestión de la infraestructura virtual

- Autenticación para administradores de la infraestructura virtual, incluyendo multifactor, con el uso de llaves iButton, eToken, JaCarta.
- Separación de los roles de los administradores de la seguridad de la información y de la infraestructura virtual, a fin de eliminar privilegios de superusuario.
- Coordinación de los cambios de configuración de la virtualización en el administrador de seguridad de la información.
- Control mandatario de acceso basado en categorías y niveles de privacidad.
- Control de acceso para los administradores de la infraestructura virtual sobre los datos que se procesan en máquinas virtuales.

Control y gestión centralizada

La consola de administración de VDP R2 permite:

- Administrar las cuentas de usuarios y permisos de acceso a los diferentes recursos.
- Implementación y configuración de los componentes de protección ESX(i)/servidores-vCenter y servidores de Hyper-V.
- Administrar la configuración de las máquinas virtuales. Visualización del historial de eventos.
- Replica online y operación en clúster.
- Integración con sistemas SIEM.

Protección contra amenazas específicas sobre entornos virtuales

- Control sobre los dispositivos virtuales.
- Control de cambios en el sistema, en base a las políticas de seguridad definidas.
- Control de integridad y booteo seguro de servidores ESX(i) y máquinas virtuales.

Auditoría y registro de eventos de seguridad

- Registro extendido de eventos relacionados con la seguridad de la información.
- Generación de informes estructurados sobre el estado del sistema y sobre los cambios producidos.
- Potente herramienta de investigación de incidentes.

ESCENARIOS DE USO

Protección de máquinas virtuales

Resultado:

- Minimizar los riesgos financieros y de reputación asociados con la copia no autorizada, la clonación, la transferencia y la destrucción de las máquinas virtuales.

Protección de las herramientas de gestión de la infraestructura virtual

Resultado:

- Las herramientas de gestión de la infraestructura virtual se encuentran dentro del perímetro protegido y cuentan con protección contra el acceso no autorizado.
- Se minimizan los riesgos de acceso no autorizado sobre la gestión de un sistema de virtualización.

Control de privilegios de los usuarios

Resultado:

- Se restringe el acceso a la gestión de la infraestructura virtual.
- Se reducen los riesgos de inoperancia del sistema debido a los daños causados por los administradores a la infraestructura virtual y a la información procesada.
- Se reducen los riesgos de pérdidas financieras debido a fugas de información, relacionados con incidentes internos.

Cumplimineto regulatorio

Resultado:

- La infraestructura virtual es un pilar fundamental en el cumplimiento de normativas como:
  - PCI DSS: Protección del secreto bancario y de información de tarjetahabientes
  - Protección de información Confidencial o Secreta en entornos militares
  - ISO 27001: Implementación de un sistema de Gestión de Seguridad de la Información
  - COBIT: Cybersecurity Framework
  - NIST Cybersecurity Framework
  - Normativas o leyes locales sobre Datos Personales

Mejoras en la gestión de seguridad

Resultado:

- Reducir del tiempo de ejecución y configuración para proteger la infraestructura virtual.
- Minimizar los riesgos financieros y de reputación basado en estándares de la industria y de las buenas prácticas internacionales.

LICENCIAMIENTO

Funcionalidad	STANDARD	ENTERPRISE
Identificatión y autenticación de los sujetos y sus permisos de acceso	✓	✓
Accesos a la gestión de la infraestructura virtual	✓	✓
Inicio de sesión segura (auditoría)	✓	✓
La información de gestión fluye entre los componentes de la máquina virtual y el perímetro	✓	✓
Máquinas virtuales confiables con control de integridad	✓	✓
La gestión del movimiento de las máquinas virtuales y de los datos procesados	✓	✓
El control de la integridad de la infraestructura virtual y sus Configuraciones	✓	✓
La división de la infraestructura virtual en segmentos	✓	✓
Crear y cargar la configuración de copia de seguridad VDP	✓	✓
Hot Standby con conmutación automática y servidor de autorización		✓
Conexión del agente de autenticación de múltiples servidores de autorización		✓
Creación de un servidor de autorización "bosque" (ajustes de sincronización entre los servidores VDP)		✓
Soporte para el modo de administración de los servidores vCenter Linked		✓
Gestión de servidor de control de Microsoft Hyper-V a través del administrador de System Center		✓
Control de aplicaciones mediante el Administrador de clústeres de conmutación		✓

SOPORTE TÉCNICO

Soporte VDP puede llevarse a cabo directamente por los especialistas del "Kod Latam Security", o a través de socios autorizados.

En el caso del apoyo técnico a través de un socio - un socio proporciona la primera línea de soporte técnico, y en el caso de incidentes complejos - por favor, póngase en contacto con el soporte técnico del proveedor.

Existen distintos niveles de soporte:

- Basico
- Estandar
- Avanzado
- VIP

CONTACTO

+598 2626 2416

World Trade Center Free Zone
Montevideo, Uruguay

info@kod.uy

www.kod.uy

KOD
LATAM
SECURITY